International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN (P): 2249–6831; ISSN (E): 2249–7943
Vol. 11, Issue 2, Dec 2021, 1–8

TRANS STELLAR
•Journal Publications •Research Consultancy

ACCESS CONTROL LISTS AND NETWORK ADDRESS TRANSLATION IN NETWORK SECURITY

MOULYA D M[1] & GEETHA V[2]

[1]*Post-Graduate Student, Department Information Science and Engineering, RV College of Engineering,*

[2]*Assistant Professor, Department Information Science and Engineering, RV College of Engineering,*

ABSTRACT

As the world of computer networks is evolving every day, the need to provide a more secure network is rapidly growing. Safe and secure communication is now needed for all organizations. Network Security is any measure taken by an organization for avoiding unauthorized usage or unintended harm to the network's private data, customers, or hardware. The aim of Network Security is to keep the network up as well as running while keeping all users secure. Network address translation is a gateway between inside and outside network. Access control lists are the rules applied on the interfaces of network devices in order to filter the traffic in the network. This paper gives a brief overview of the contribution of network address translation and access-control lists in maintaining the security of the organization's network.

KEYWORDS: Access-control lists, Network address translation, Network security.

Received: May 15, 2021; **Accepted:** Jun 05, 2021; **Published:** Jun 24, 2021; **Paper Id.:** IJCSEITRDEC20211

Original Article

INTRODUCTION

The organizational network size, their number of users as well as complexity, have rapidly raised in recent years. This enormous increase in growth makes it very difficult to provide the network with security. Network security is the key problem of computer networking systems and services implementation and operation as various types of attacks are growing day by day. The crucial question is how these computer network systems as well as services should be protected against malicious nodes that cause many issues within the network environment including the unavailability of services, data losses and privacy in communications. Until properly protected, every network is responsive to unintended and malicious use. Personal data, such as business secrets and personal records, may be disclosed by hackers, unfortunate staff or bad security procedures inside the company. For example, a loss of confidential research will theoretically cost the company millions of dollars by losing advantage of strategic advantages. As hackers intercept and sell consumer data for fraud, misleading advertising and public misconceptions of the organizations are created.

The majority of typical network attacks are aimed at gaining access to information by hacking on conversations and user data instead of damaging the network itself. However, attackers could do more than steal files. They will destroy the devices of users or manipulate systems for physical access to facilities. This puts the property and the members of the organization at risk of harm. Competent network security processes protect the data from external interference and block vulnerable systems. This enables users of the network to stay safe as well as focus on accomplishing the objectives of the organization.

2. ACCESS-CONTROL LIST

A network filter is used to authorize and limit data flows to and from network interfaces through network equipment such as the firewalls, routers and switches. The network system analyses data flowing through the interface where an access control list has been configured on an interface, compares the data with conditions specified in the lists, as well as enables data to flow or forbids it.

The primary reason for access-control list is for providing a basic security level for the network. The limited complexity and ease of use of operation of stateful firewalls may not permit the use of higher- the allowance of higher speeds on fast interfaces, though the level of security on these firewalls is reduced. They also limit changes for network peers to route, which can help to define network traffic flow control.

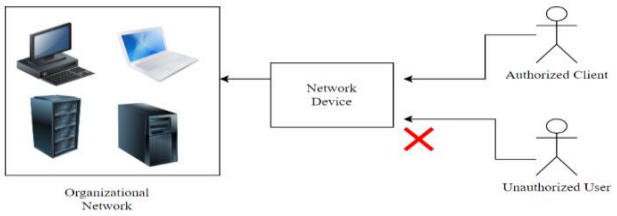

Figure 1.1: Access Control Lists

In the figure, there are authorized clients and also unauthorized user whose access to the organization network is denied.

Types of ACL

In relation to two key sections, lists of access control may be approached:

- **Standard ACL**

A list of accesses developed only with the source IP address. Such access control lists cause the entire protocol suite to be blocked. They don't distinguish between TCP, UDP along with HTTPS IP traffic. They utilize numbers 1-99 or 1300-1999 in order to allow the router to identify the address as the IP source.

Syntax:

access-list [1-99] [permit | deny] [source address] [wildcard mask]

- **Extended ACL**

An IP traffic differentiating access list which is often used. This utilizes IP addresses and port numbers for IP traffic both at the source and the destination. You may also indicate what IP traffic is permitted or refused. The figures 100-199 and 2000-2699 are used.

Syntax:

access-list [100-199] [permit | deny] [protocol] [source address] [wildcard mask] [destination address] [wildcard mask] [operator] [port]

There are 2 more types of ACL as well:

- **Named ACL**

Named access lists offer two advantages. First, for documentation reason, we should use a recognizable name in an access list. Second, in a named access list, we will exclude individual lines that cannot be included for numbered access lists.

- **Numbered access list**

The access list should not be removed after it is produced, i.e., in case of the numbered access list, it is not possible to delete a provision from an access list. This is the access list that is not allowed. The entire list of accesses will be deleted if we attempt to remove a provision from the access list. With regular and expanded access list, the numbered access list could be used.

3. NETWORK ADDRESS TRANSLATION (NAT)

Not many domestic places had more than a PC a decade back. However, this is now almost necessary for many people to have two or three personal Computers. At the time, a small part of home computer users subscribed to was ADSL or the Internet over a cable. At present, these broadband networks are increasingly subscribed by users.

With the extreme development of the internet as well as associated networks in mind, the allocation of IP address is a biggest challenge. The issue of the absence of IP addresses has been initial just a theoretical one, which would occur in the far future. So, here's the future! The issue is no longer theoretical - this is happening right now. More and more people began to need public IP addresses permanently, which added to the trouble and required a fast solution.

This solution came with Port Address Translation (PAT), Network Address Translation (NAT). An entirely new address system, known as IPv6, has to be used with more confident and effective approach, with 128 bits instead of the 32 found in IPV4.

The Network Address (NAT) translation procedure involves the assignment of a computer public address (or group of computers) to a network system within an interconnected network, typically a network device. NAT is mostly to restrict the number of public IP addresses a business or entity must use for both cost-effectiveness and security and automation tests. NAT is a mechanism for modifying the IP addresses and ports of source and destination. The need for public IPv4 addresses restricts Address translation and masks private address set of the network. It is normally performed by firewalls or routers.

There are three types in NAT:

- **Static NAT**

One-to-one mapping is provided by Static NAT between global as well as local addresses, therefore, a single IP address must be assigned to any network device.

- **Dynamic NAT**

The router is equipped with a pool of routable IP addresses, and the router transfers addresses from that pool to each computer requiring "outside world" traffic. This kind of NAT requires good plan from its inception so that the pool of IP addresses is sufficient to meet the network requirements of the Internet peak time traffic.

- **PAT**

Translation of the port address is another and most common version of the NAT. This is also named NAT Overload since the application of the various ports addresses on the UDP or TCP directory will map several private IP addresses to only one registered IP address (overloaded address).

Due to some security constraints business organizations started with two more types of NAT:

- **Private IP to Private IP NAT**

In this type of NAT one private IP is mapped to other private IP. This is done to protect the privacy of both the network. In this case NAT acts as a gateway between two private networks.

- **Identity NAT**

In identity NAT the real address is mapped to itself, this is done in order to make sure that only authorized network can initiate communication with the other network.

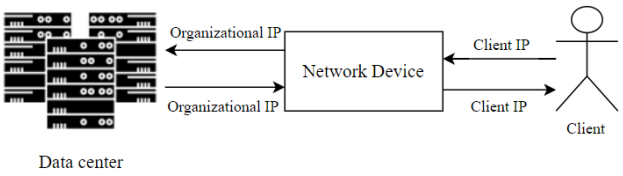

Figure 1.2: Access Control Lists

In the above figure, to access the services in Data center client-side IP has to be changed to organization side IP.

4. PREVIOUS WORK

IPV4 address will get exhausted as it is finite. There were two solutions to this problem:

- To expand the size of the address which became IPv6. This was a long-term solution.
- To temporarily solve the problem NAT technique was introduced. The smaller subset called private address were formed from the superset IPv4. Private addresses were not globally unique.

Hence, these private addresses were mapped to public address to communicate with internet. Simulation of NAT in organizations has showed that NAT eases network administration.

With the drastic network growth, ACL will become very important to monitor it. Every packet a network device receives is evaluated against the rules applied on the devices. Only if the criteria match the packet is allowed to flow or else it is dropped. Deployment of ACL is very important in organization network to monitor each and every flow in network.

5. ROLE OF ACL AND NAT IN NETWORK SECURITY

The network interface passes all traffic sent by it by chance, with no constraints. ACL is a mechanism that can be used to specify which node or IP to provide access to the internal network and vice versa for external networks. The access control function is performed on an OSI layer lower than the proxy gateway, which makes it less complicated. A portal to filter a packet is also much quicker than its cousins.

ACL allows or denies statements consist essentially of IP addresses and ports for the source as well as the destination.

A statement allowing the ACL permission enables access to the required IP address/network destination address/specified. On the other hand, the ACL statements are denied. The firewall inserts an implicated DENY ALL assertion rule at the end of the ACL that is not available in the setup by default. Once the ACL is applied and the packet is filtered, only the traffic permitted will enter into the other side of the network.

NAT is mapping of one IP address space to other IP address space. Security as well as privacy can be provided by NAT. Since NAT transfers data packets from one IP to another, this also prevents access to a private interface for something else. The network machines sort the data to make it more complicated for unintended data to get in. This isn't stupid, but it also serves as your device's first protection.

Consider ACL and NAT as the company's old mailroom. Receipt parcels to the company address are checked and the mailroom attaches the cube number of the receiver for inside delivery. Simply discarding packages coming without a valid receiver. Outbound packages travel to the corresponding postal carrier or shipper via the mailroom. For inbound or outbound packets, NAT executes a similar function.

Now to the mailroom add a security element. Packages received from an x-ray system and bomb procedure are being used. In order to ensure no harmful or forbidden objects, the content shall be reviewed. It is possible to search the return address and block it if the shipment originates from a given address or location. After passing thru the security, the post office attaches the number of the receiver to be sent. Packages that are outbound are still running after stability. Blocking and returning the packs to the internal sender for some addresses or containing any of the objects. His director gets a report on what was and why blocked. This is the feature of an incoming and outgoing firewall package.

ACLs conduct stateless controls, such that the permission list examines a packet and does not know what has happened. If an ACL checks a packet with an ACK bit collection using TCP, the ACL may only acknowledge that it is an acceptance packet.

6. CONCLUSIONS

To achieve security in an organizational network is very difficult. Configuring hardware devices accurately based on the security requirements is one of the prime components in maintaining a secure network. There are advanced security policies today, but still providing security at basic level becomes very important too. This way attacks can also be brought into light at the rudimentary level only. To provide efficient network security for an organization, there should be a firewall which blocks the traffic that can be harmful. Network devices should be configured with ACL in order to keep the traffic flow precise. NAT provides acts as a gateway between inside and outside network.

REFERENCES

1. *Zhang, L., 2008. A retrospective view of network address translation. IEEE network, 22(5), pp.8-12.*
2. *Samociuk, D., B. Adamczyk, and A. Chydzinski. "Impact of router security and address translation mechanisms on the transmission delay." In Proc. 7th International Conference on Evolving Internet (INTERNET 2015), pp. 38-42. 2015.*
3. *"Access Control List" Nahush Kulkarni, Harsh Kothari, Hardik Ashar, Sanchit Patil in International Journal for Research in Applied Science & Engineering Technology (IJRASET), IC Value: 13.98 ISSN: 2321-9653*

4. *Bansal, Anchit, and Priyanka Goel. "Simulation and Analysis of Network Address Translation (NAT) & Port Address Translation (PAT) Techniques." Int. Journal of Engineering Research and Application 7, no. 7 (2017): 50-56.*
5. *Zheng, S., Li, Z. and Li, B., 2017, March. Implementation and application of ACL in campus network. In AIP Conference Proceedings (Vol. 1820, No. 1, p. 090014). AIP Publishing LLC.*
6. *Mihăilă, P., Bălan, T., Curpen, R. and Sandu, F., 2017. Network Automation and Abstraction using Python Programming Methods. MACRo 2015, 2(1), pp.95-103.*
7. *Farooq, Umer. (2018). Network Security Challenges. 10.13140/RG.2.2.27478.34885.*
8. *Sharma, S. and Khadke, M., 2018, December. Network Security: A Major Challenge in India. In 2018 4th International Conference on Computing Communication and Automation (ICCCA) (pp. 1-5). IEEE.*
9. *Gedia, D. and Perigo, L., 2018. A Centralized Network Management Application for Academia and Small Business Networks. In Information Technology in Industry Journal (Vol. 6, No. 3, pp. 1-10). ITII.*
10. *Soni, Anshu, and Virender Ranga. "API Features Individualizing of Web Services: REST and SOAP." International Journal of Innovative Technology and Exploring Engineering 8 (2019): 664-671.*
11. *Neumann, A., Laranjeiro, N. and Bernardino, J., 2018. An analysis of public REST web service APIs. IEEE Transactions on Services Computing.*
12. *Ruambo, Francis. (2019). Network Security: A Brief Overview of Evolving Strategies and Challenges. International Journal of Science and Research (IJSR). 8. 834-841. 10.21275/ART20194980.*
13. *Bush, Steven M., Thomas C. Butcher, Matthew Tebbs, Justin Ferrari, Brett Marl, Ron Gery, Kristin Acker, and Joshua Hinds. "Network management." U.S. Patent 7,925,729, issued April 12, 2011.*
14. *Sprecher, J.W., Winters Jr, D.J., Rajwany, A.S., Dodson, M.W., Penning, G.R., Harrington, D.F. and Chou, S., Pactel Corp, 1994. Network management system. U.S. Patent 5,285,494.*
15. *Henderson, G.S., Perry, W.B., Franklin, T.D., Sanders Jr, E.J. and Cooley, V.A., MCI Corp, 1998. Network management system. U.S. Patent 5,726,979.*
16. *Egevang, Kjeld, and Paul Francis. The IP network address translator (NAT). RFC 1631, may, 1994.*
17. *Tang, P., Diep, T. and Hlasnik, W., Intel Corp, 2006. Access control management system utilizing network and application layer access control lists. U.S. Patent 7,054,944.*
18. *Gemünden, H.G., Ritter, T. and Heydebreck, P., 1996. Network configuration and innovation success: An empirical analysis in German high-tech industries. International journal of research in marketing, 13(5), pp.449-462.*
19. *Marin, G.A., 2005. Network security basics. IEEE security & privacy, 3(6), pp.68-72.*
20. *Dotcenko, S., Vladyko, A. and Letenko, I., 2014, February. A fuzzy logic-based information security management for software-defined networks. In 16th International Conference on Advanced Communication Technology (pp. 167-171). IEEE.*
21. *Ghosh, Ramkrishna. "An efficient and robust modified RSA based security algorithm in modern cryptography." J Comput Sci Eng Inform Technol Res (JCSEITR) 6.2 (2016): 15-22.*
22. *Bishoi, TANMOY KUMAR, RAMKRISHNA GHOSH, and TANMOY SINHA ROY. "An algorithm on text based security in modern cryptography." J Comput Netw Wirel Mobile Commun 5.1 (2015).*
23. *Kapadia, GAYATRI SHITANSHU, and RAVI M. Gulati. "Security concern for virtualization in cloud computing." International Journal of Computer Science Engineering and Information Technology Research 4.5 (2014): 107-116.*

24. *Gavhane, Sachin Prakash, and Vijay Maruti Shelake. "Intrusion Detection System Using Optimal C4. 5 Algorithm." Int. J. Comput. Sci. Eng. Inf. Technol. Res. 4.2 (2014): 5-14.*

25. *Devi, S. Gayathri, Dr A. Marimuthu, and Dr A. Kavitha. "Multicast Routing in Mobile Ad Hoc Networks: Issues and Techniques." International Journal of Computer Science and Engineering 3.3 (2014): 1-8.*